Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (cancelled)

2. (not presented)

3. - 8. (cancelled)

9. (currently amended) A method of performing a transaction in a communication system between a first and a second participant wherein said second participant permits a service to be provided to said first participant in exchange for a payment, said method comprising the steps of:

a) upon initiation of said transaction by said first participant, said second participant sending a first message to said first participant, said first message including information pertaining to said second participant;

[[a)]] b) said first participant verifying ~~the legitimacy of~~ said information pertaining to said second participant to obtain assurance that said service will be provided upon assuring said payment;

c) said first participant sending a second message to said second participant, said second message including information pertaining to said first participant;

[[b)]] d) said second participant verifying ~~the legitimacy of~~ said information pertaining to said first participant to obtain assurance that payment will be secured upon provision of said service; and

[[c)]] e) upon verification of said information pertaining to said first participant, said second participant obtaining a digital signature for said first participant on said transaction using said second message, whereby said second participant may obtain said payment from a third participant using said digital signature.

10. (previously presented) A method according to claim 9 wherein said first participant is a holder of a card which performs cryptographic operations.

11. (previously presented) A method according to claim 10 wherein said second participant is a terminal.

12. (previously presented) A method according to claim 11 wherein said third participant is a financial institution.

13. (currently amended) A method according to claim 9 wherein ~~step (a) further comprises:~~

~~i) said second participant sending a first message to said first participant, the first message including~~ said information pertaining to said second participant included in said first message includes details and credentials of said second participant; and said first participant verifies said details and said credentials in step b).

~~ii) said first participant said transaction details and said credentials.~~

14. (currently amended) A method according to claim [[13]] 9 wherein ~~step (b) further comprises:~~

~~i) said first participant sending a second message to said second participant, said second message including~~ said information pertaining to said first participant included in said second message includes details and credentials of said first participant; and said second participant verifies said details and credentials in step d).

~~ii) said second correspondent verifying said credentials of said first participant.~~

15. (currently amended) A method according to claim [[14]] 9 wherein said second message includes a challenge and step [[(c)]] e) further comprises:

i) said second participant generating a response to said challenge;

ii) said second participant sending a third message including said response to said first participant;

iii) said first participant verifying said response; and

iv) said first participant sending a fourth message to said second participant such that said

digital signature is provided by said second message and said fourth message.

16. (currently amended) A method according to claim 15 further comprising:

i) said second participant verifying information in said fourth message;

ii) said second participant completing said transaction by providing said service; and

iii) said second participant sending said third participant a subset of said first, second, third and fourth messages to obtain said payment.

17. (currently amended) A method according to claim 16 further comprising:

i) said third participant verifying said subset;

ii) said third participant providing said payment to said second participant.

18. (previously presented) A method according to claim 13 wherein said credentials include a public key certificate.

19. (previously presented) A method according to claim 15 wherein said challenge is a nonce.